THINKDIGITAL
INNOVATIVE SOLUTIONS PROVIDER

NAC R1

Manual de Configuração e Utilização

Manual de Configuração/Utilização

Manual de Configuração, Utilização e Boas Práticas para a integração de equipamentos de rede NAC em ambientes de produção empresariais.

Primeiro Trimestre 2011 – ThinkDigital – *versão do documento v0.1*

WWW.THINKDIGITAL.PT

2011

THINKDIGITAL
HQ – Rua Cristóvão Pinho Queimado, nº65
MIRADOR BUSINESS CENTER
Aveiro – Portugal
Tf: +351 234 197 149
Fx: +351 234 197 562
www.thinkdigital.pt

ThinkDigital NAC

Este manual ilustra como configurar e utilizar as funcionalidades do servidor Network Admission Control da ThinkDigital, NAC R1, passo-a-passo tendo como objectivo uma demonstração dos procedimentos correctos para a sua configuração, utilização e integração numa rede empresarial moderna.

Antes de avançar para a explicação das múltiplas funcionalidades, é especialmente aconselhado a leitura da secção “Visão Geral” para um melhor entendimento do servidor NAC.

Conteúdo

1. Visão Global 3
1. Equipamento 3
2. Configuração de Rede 4
3. Iniciar Sessão WEB 6
4. Alteração da Palavra-Chave 7
5. Menu NAC 8
5.1. Criar conta residente 8
5.2. Criar e Configurar um Perfil Local 10
5.3. Criar e Configurar uma Conta Convidado 12
5.4. Configurar Autoridades 16
5.5. Configurar Banner da Página Principal 22
5.6. Opções Politicas de Acesso 20
6. Menu Firewall 23
6.1. Configurar Tráfego Autorizado e Não Autorizado 23
6.2. Criar Redireccionamentos 24
6.3. Dispositivos Privilegiados e Dispositivos Excluídos 25
7. Menu Serviço RADIUS 26
8. Menu Proxy HTTP 27
9. Menu Reverse Proxy 29
10. Menu Serviço DHCP 30
11. Menu Serviço DNS 32

1. Visão Global

O NAC é um sistema de controlo de acesso á rede com administração centralizada que permite uma simples e intuitiva gestão de perfis, utilizadores, acesso a sites, largura de banda entre outros. Além da visualização de estatísticas de tráfego, o NAC regista todos os acessos á rede ajudando-o a manter-se em conformidade com o novo decreto de lei 32/2008. O NAC é compatível com qualquer sistema operativo, basta possuir uma placa de rede para se ligar á rede e o NAC entrará em acção, sem qualquer necessidade de configurações por parte dos computadores pessoais.

O NAC possui uma proxy transparente que faz cache dos conteúdos acedidos, acelerando pedidos posteriores aos mesmos conteúdos e também diminuindo o uso de largura de banda e tráfego. A proxy também pode filtrar pedidos das máquinas para bloquear acesso a websites. Por ser uma proxy transparente só e necessário configurações por parte do NAC.

O NAC permite adicionar 3 tipos de servidores de autenticação: controladores de domínio, servidores RADIUS ou servidores NAC. Assim será possível aos utilizadores desses servidores utilizarem as suas credenciais para se autenticarem no NAC.

O NAC também disponibiliza um serviço DHCP simples e prático em caso de não possuir outro sistema para o fazer. O serviço DHCP serve atribuir automaticamente um IP às maquinas que se liguem á rede e restantes configurações necessárias para tal.

Portanto o NAC é uma ferramenta essencial para um eficiente controlo da rede da sua empresa que é administrado através de um interface WEB2.0, sendo por isso acessível em qualquer parte através de um simples Web-browser de forma rápida e intuitiva.

1. Equipamento

Antes de montar o seu equipamento na sua infra-estrutura leia com atenção todos os pontos referidos neste capítulo.

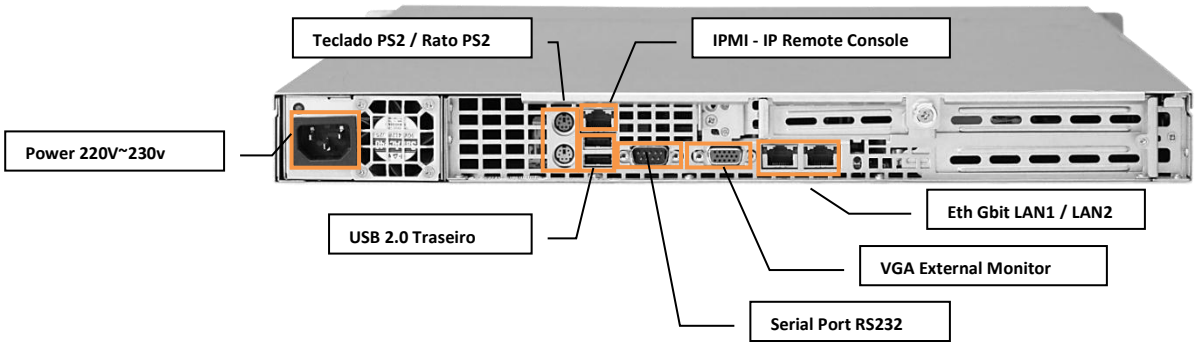
Características Técnicas e Funcionamento

Modelo do Equipamento	HES – 1U RACK
Alimentação / Energia	220V ~230v AC
Consumo Médio	~90W
Comunicação em Rede	2x 1Gbit/s Ethernet Card
Comunicação USB	4x USB 2.0
Gestão Local de Emergência	VGA + PS2 Teclado e Rato
Gestão Remota	WEB / SSH / IPMI

NOTA! Deverá garantir uma alimentação redundante/socorrida por baterias, utilizando para isso uma unidade externa de UPS (Uninterruptible Power Supply)

Painel Frontal:

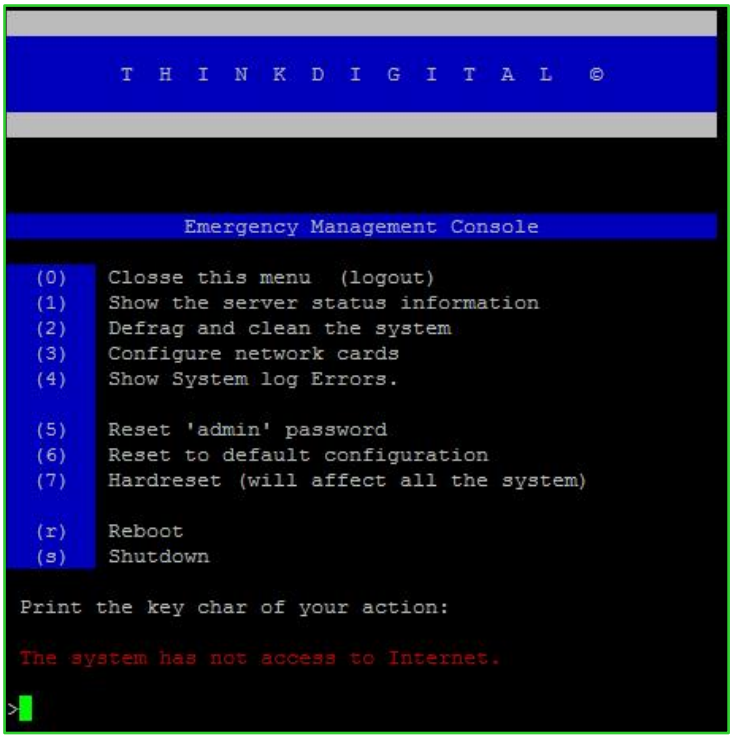
Painel Traseiro:



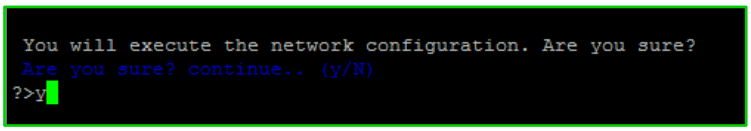
Recomendações Montagem: Ao montar o seu equipamento no bastidor deverá ter em consideração o fácil acesso ao painel superior do equipamento, tipicamente utilizado para efectuar actualizações da unidade "flash" que contem o firmware do sistema operativo.

2. Configuração de Rede

O endereço IP por omissão do NAC é o "192.168.0.x", porém pode ser configurado na *"Emergency Management Console"* em caso da impossibilidade de acesso através da ligação de rede existente na organização. Para configurar o equipamento, ligue um teclado e um monitor ao NAC e inicie uma sessão com o utilizador "**thinkdigital**" e palavra-chave "**thinkdigital**". Após a introdução correcta das credências de acesso, o sistema irá mostrar-lhe um menu de configuração rápida de sistema, como é ilustrado na figura seguinte. Neste especifico caso, para configurar a rede pressione a tecla "**3**" e de seguida a tecla "**Enter**":

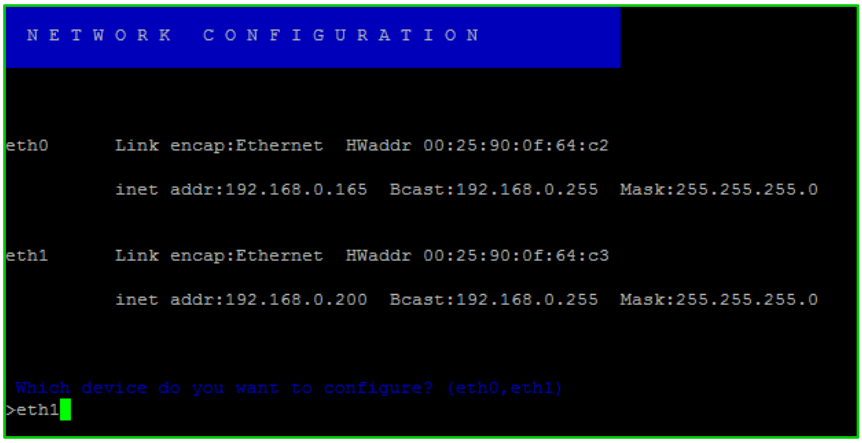

T H I N K D I G I T A L ©
Emergency Management Console
(0) Closse this menu (logout)
(1) Show the server status information
(2) Defrag and clean the system
(3) Configure network cards
(4) Show System log Errors.
(5) Reset 'admin' password
(6) Reset to default configuration
(7) Hardreset (will affect all the system)
(r) Reboot
(s) Shutdown
Print the key char of your action:
The system has not access to Internet.
>

Pressione a tecla “**y**” para confirmar a opção escolhida e de seguida pressione a tecla “**Enter**” para confirmar:

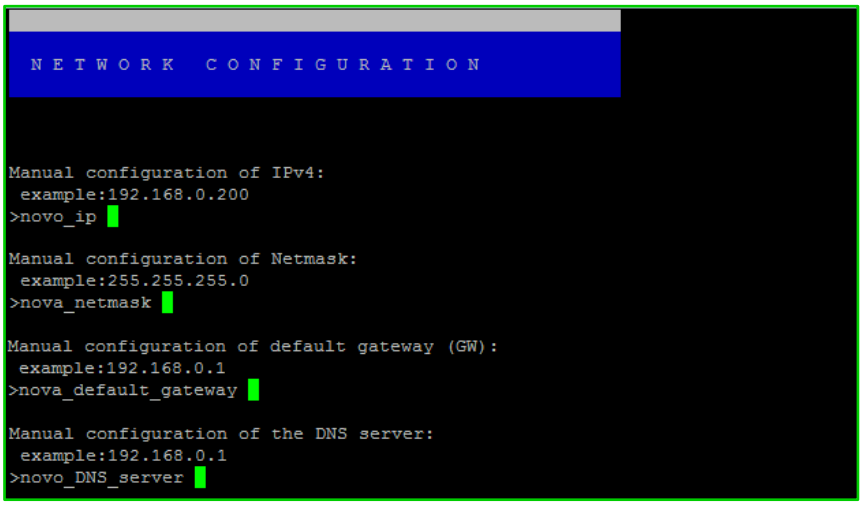


Tal como ilustra na figura seguinte, escolha o interface a configurar, neste caso seria escrever “**eth1**” e pressionar a tecla **Enter**.

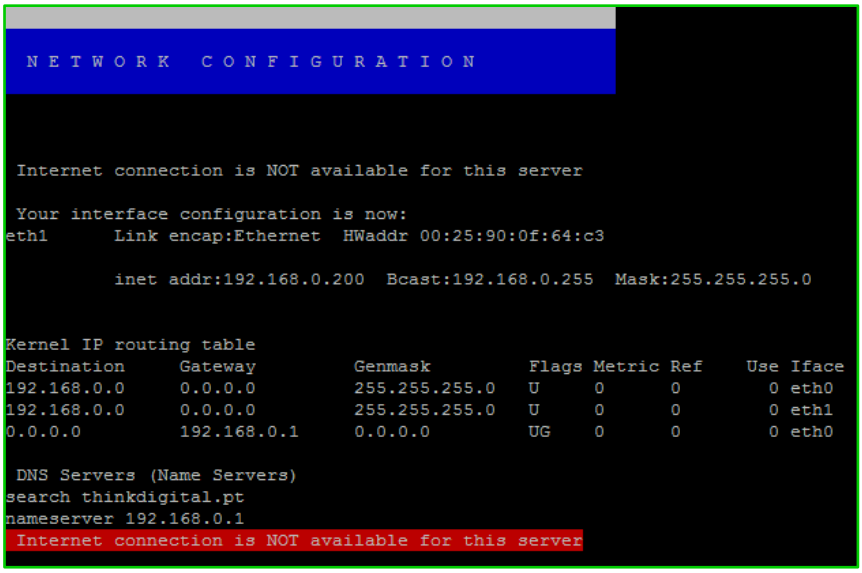
ALERTA! Note que o nome interface depende directamente onde tem o cabo de rede ligado no seu servidor!


N E T W O R K C O N F I G U R A T I O N
eth0 Link encap:Ethernet HWaddr 00:25:90:0f:64:c2
inet addr:192.168.0.165 Bcast:192.168.0.255 Mask:255.255.255.0
eth1 Link encap:Ethernet HWaddr 00:25:90:0f:64:c3
inet addr:192.168.0.200 Bcast:192.168.0.255 Mask:255.255.255.0
Which device do you want to configure? (eth0,eth1)
>eth1

Seguidamente, introduza o novo endereço IPv4 que pretende usar no seu NAC, compatível com a sua rede existente, máscara, default gateway e DNS server. (Ver figura seguinte).



Finalizando, tal como ilustra a figura seguinte, o sistema mostra as configurações aplicadas. Neste momento deverá conseguir iniciar uma sessão WEB para aceder á gestão do NAC através do endereço IPv4 definido.

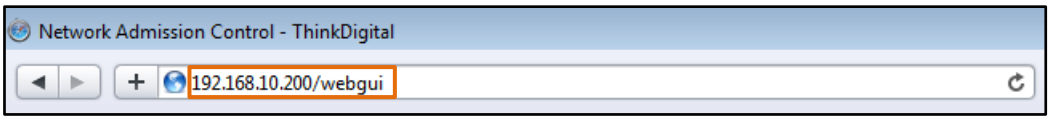

NETWORK CONFIGURATION
Internet connection is NOT available for this server
Your interface configuration is now:
eth1 Link encap:Ethernet HWaddr 00:25:90:0f:64:c3
inet addr:192.168.0.200 Bcast:192.168.0.255 Mask:255.255.255.0
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
0.0.0.0 192.168.0.1 0.0.0.0 UG 0 0 0 eth0
DNS Servers (Name Servers)
search thinkdigital.pt
nameserver 192.168.0.1
Internet connection is NOT available for this server

IMPORTANTE: Deverá garantir que o seu equipamento tem acesso à Internet. Sem o acesso à Internet o seu equipamento não será capaz de calcular as credenciais de validação de segurança do seu firmware e irá bloquear o seu funcionamento após algumas horas e tentativas falhadas. Para situações onde não seja de todo possível ter acesso à Internet, deverá contactar a THINKDIGITAL e solicitar apoio nesse problema.

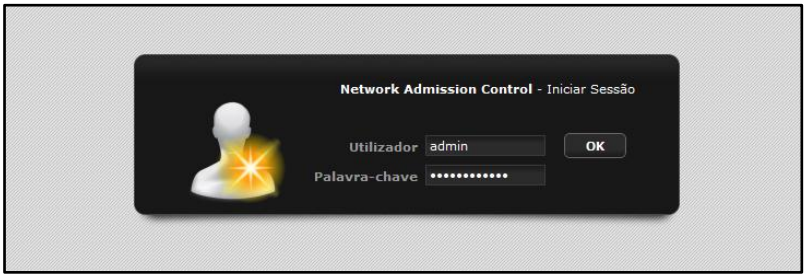
3. Iniciar Sessão WEB

Para aceder á gestão do NAC basta utilizar um Web-Browser moderno. O Browser escolhido deverá ser o mais compatível possível com as normas definidas pelo consórcio WorldWide Web Consortium (W3C) para ser possível a utilização a 100% das capacidades gráficas deste interface de gestão WEB.

De forma a aceder, deverá digitar o endereço do NAC com o sufixo "/webgui" no Browser e pressionar a tecla "**Enter**", tal como ilustrado na figura seguinte.

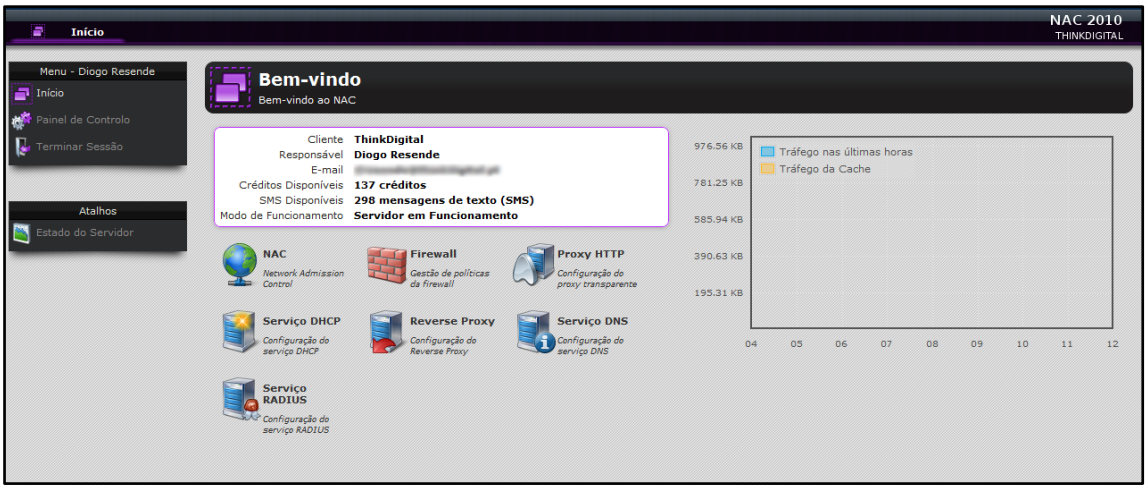


Posteriormente deverá indicar as suas credenciais de acesso para aceder ao painel de administração.



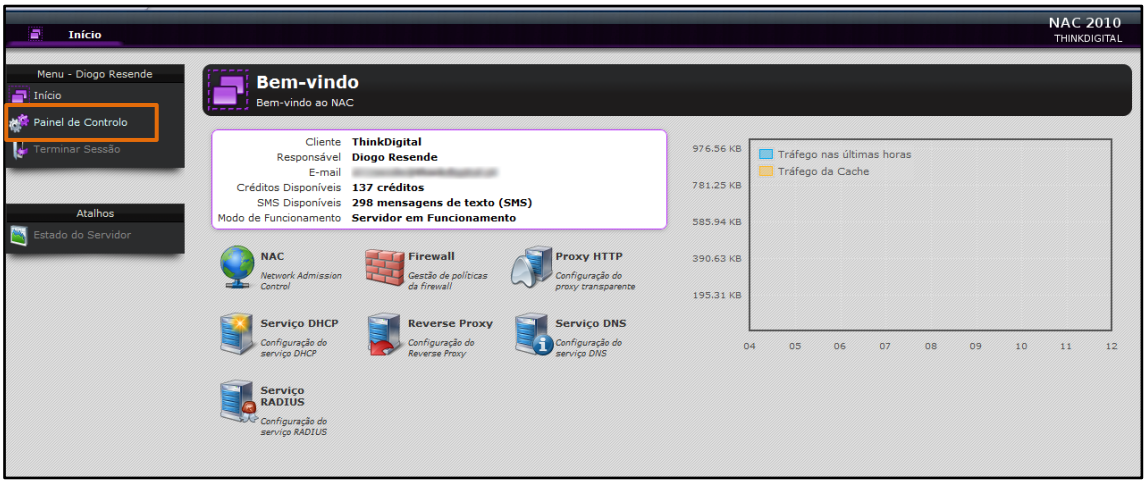
IMPORTANTE: Por omissão o utilizador é "admin" e a palavra-chave é "thinkdigital", pelo que é extremamente aconselhável mudar a palavra-chave de seguida.

Na figura abaixo pode se observar o ecrã de início do NAC:



4. Alteração da Palavra-Chave

Comece por seleccionar a opção **“Painel de Controlo”** no menu “**Administrador**”:

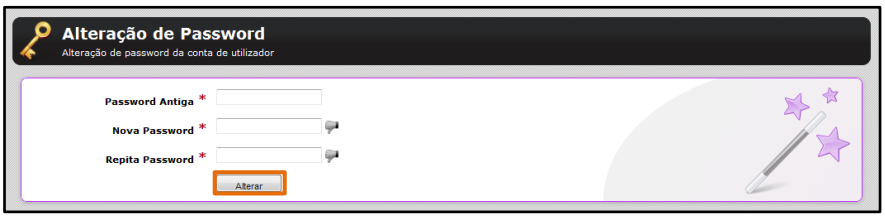


Seguidamente seleccione a opção “**Utilizadores e Preferências**” no menu “**Categorias**”.

Seleccione a opção “**Definições Pessoais**”:

Escolha a opção “**Palavra-chave**”:

E por fim, poderá definir a nova palavra-chave, tal como ilustra na figura seguinte.

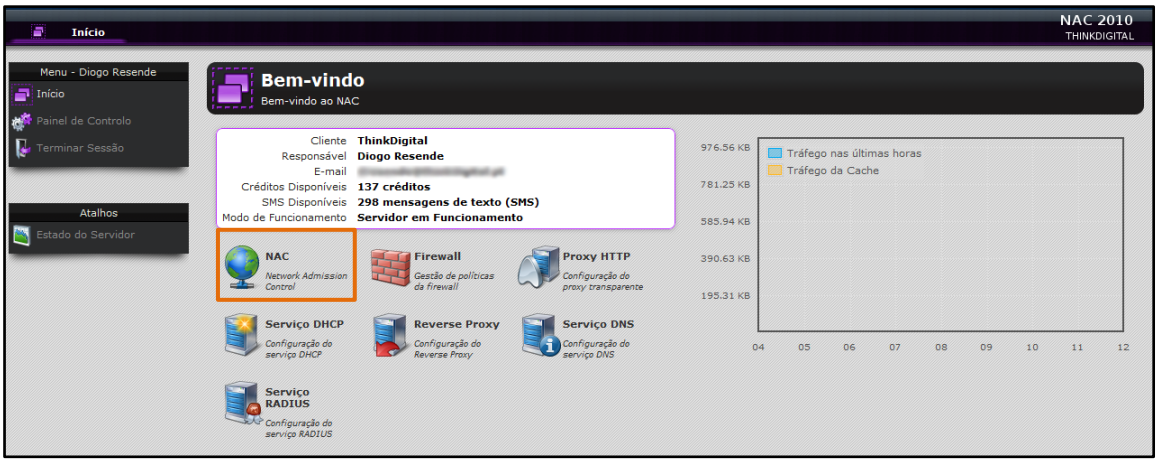


5. Menu NAC

No menu NAC é possível configurar por exemplo contas de utilizador e políticas, ver estatísticas de tráfego, ver histórico das ligações ou ver que utilizadores estão online.

5.1. Criar conta residente

Uma conta residente é destinada a utilizadores “fixos”, ou seja, utilizadores que precisarão de acesso contínuo aos recursos providenciados pela rede. Na conta residente é possível aplicar políticas de acesso á rede através de perfis locais, explicado posteriormente. Para criar uma conta residente comece por seleccionar a opção “NAC” no ecrã “Início”:

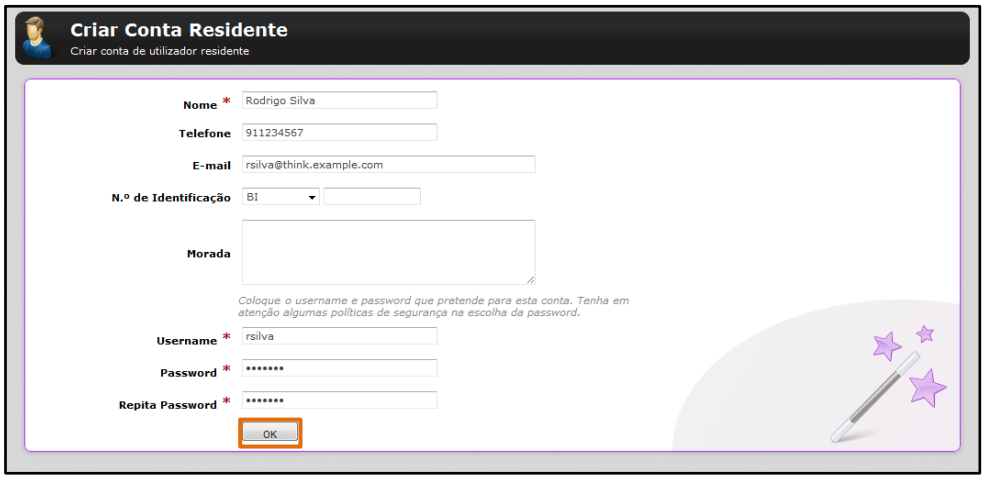


Seleccione a opção “Politicas de Acesso” no ecrã “NAC”:

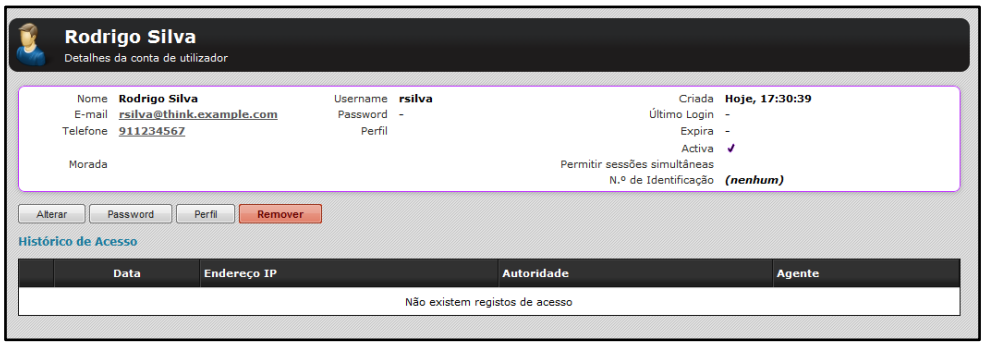
De seguida seleccione a opção “Contas Locais” no ecrã “Políticas de Acesso”:

Por fim, no ecrã “Contas Locais” seleccione a opção “Criar Conta Residente” no menu “Atalhos”:

No ecrã “Criar Conta Residente” depois de todos os campos necessários preenchidos correctamente clique no botão “Ok” para finalizar:



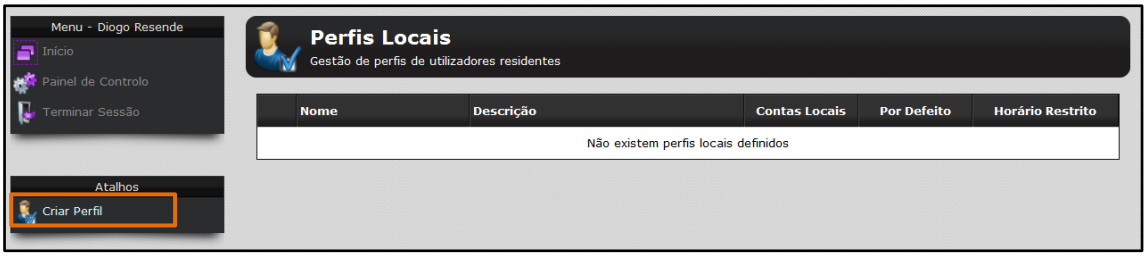
Neste ecrã podemos verificar todas os parâmetros definidos para este utilizador assim como opções para a gestão do mesmo:



5.2. Criar e Configurar um Perfil Local

No perfil local é possível a configuração de políticas de acesso á rede para de seguida aplicar aos utilizadores desejados. Desta forma, pode aplicar restrições a um conjunto de utilizadores de uma forma simples, eficaz e rápida. Para criar um perfil local, seleccione a opção “NAC” no ecrã de início, de seguida seleccione a opção “Políticas de Acesso” e por fim seleccione a opção “Perfis Locais”:

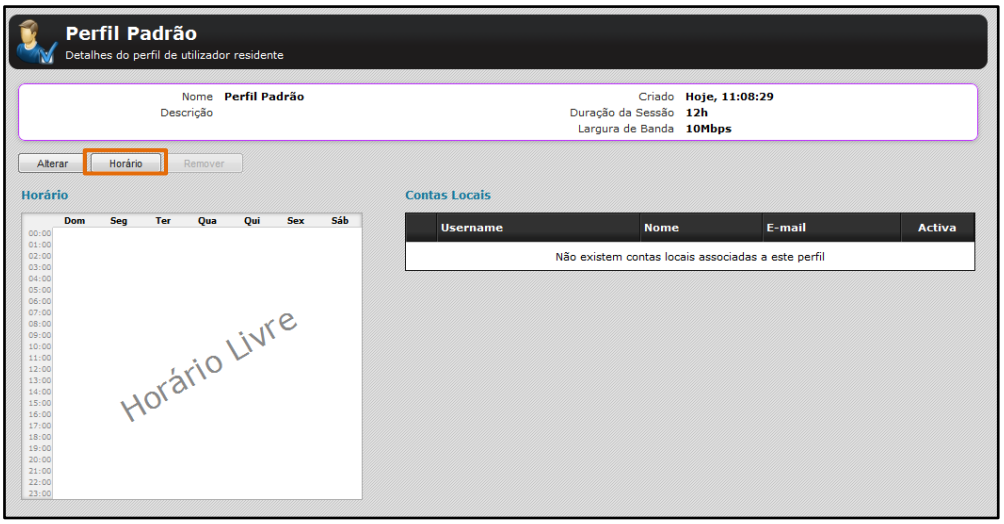
No ecrã “Perfis Locais”, seleccionar a opção “Criar Perfil” no menu “Atalhos” como mostra a imagem abaixo:



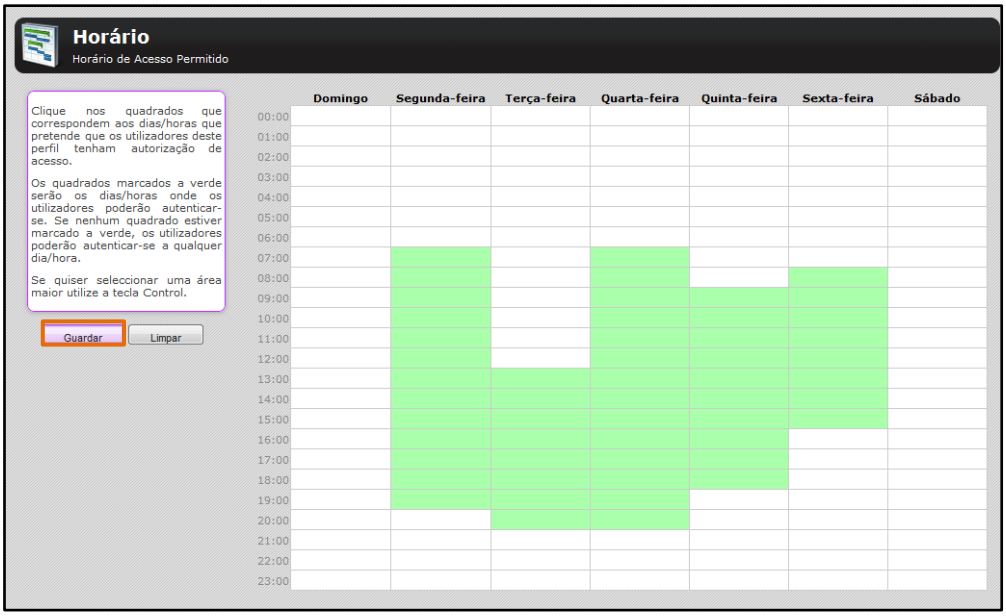
De seguida preencha todos os campos correctamente e clique no botão “Ok” para terminar. Se pretender que este perfil seja aplicado por omissão a todos os utilizadores residentes, seleccione a opção “Perfil por defeito utilizado para novas contas locais” como indicado na imagem abaixo:

Criar Perfil
Criar perfil de utilizador residente
Nome *
Perfil Padrão
Descrição
Perfil por defeito utilizado para novas contas locais
A duração é calculada a partir do momento que o utilizador iniciar sessão. Utilize as letras 'h' para horas ou 'd' para dias.
Duração da Sessão *
12h
A largura de banda corresponde teoricamente à velocidade máxima conseguida pelos utilizadores do perfil. Utilize as unidades de medida Kbps ou Mbps se pretender (a unidade é em bits por segundo). Se não pretender um limite, coloque apenas um hífen no campo seguinte.
Largura de Banda
10mbps
OK

Depois do perfil criado, é-lhe mostrado todos os detalhes do perfil. Se quiser restringir os utilizadores residentes deste perfil para se autenticarem exclusivamente em determinados dias/horas, clique no botão “Horário”:



Para seleccionar uma hora num determinado dia em que os utilizadores poderão autenticar-se, clique no quadrado dia/hora correspondente. A cor verde indica que esse dia/hora o utilizador poderá autenticar-se. Por omissão, se nenhum quadrado estiver seleccionado, os utilizadores poderão autenticar.se em qualquer altura. Para acelerar o processo de escolha das horas, poderá utilizar a tecla “Control” para seleccionar uma maior área de quadrados. Para finalizar, clique no botão “Guardar”:

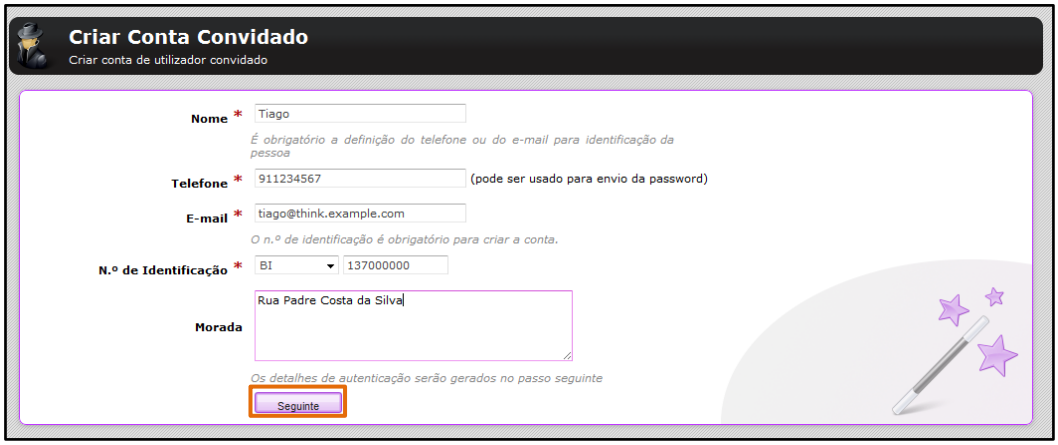

Horário
Horário de Acesso Permitido
Clique nos quadrados que correspondem aos dias/horas que pretende que os utilizadores deste perfil tenham autorização de acesso.
Os quadrados marcados a verde serão os dias/horas onde os utilizadores poderão autenticar-se. Se nenhum quadrado estiver marcado a verde, os utilizadores poderão autenticar-se a qualquer dia/hora.
Se quiser seleccionar uma área maior utilize a tecla Control.
Guardar
Limpar
Domingo
Segunda-feira
Terça-feira
Quarta-feira
Quinta-feira
Sexta-feira
Sábado

Se não seleccionar um perfil na criação de novos utilizadores, este perfil será aplicado automaticamente. Se quiser aplicar este perfil a um utilizador já existente, volte ao ecrã “Contas Locais”, seleccione o utilizador que pretende alterar, e nos detalhes do utilizador clique no botão “Perfil”. No ecrã “Alterar Perfil”, seleccione o perfil desejado e clique no botão “Ok”.

5.3. Criar e Configurar uma Conta Convidado

Uma conta de utilizador convidado tem como propósito para dar acesso temporário na rede a pessoas usualmente exteriores á empresa. Este tipo de contas pode ter data ou tempo de expiração para assim o NAC automaticamente desactivar as contas. Esta funcionalidade do NAC permite-lhe aumentar o controlo sobre os utilizadores convidados e a manter-se em conformidade com o decreto de lei 32/2008. Para criar uma conta convidado seleccione a opção “Políticas de Acesso” no ecrã “NAC”, depois seleccione “Contas Locais”, por fim seleccione a opção “Criar Conta Convidado” no menu “Atalhos”:

De seguida preencha todos os campos correctamente e clique no botão “Seguinte”:

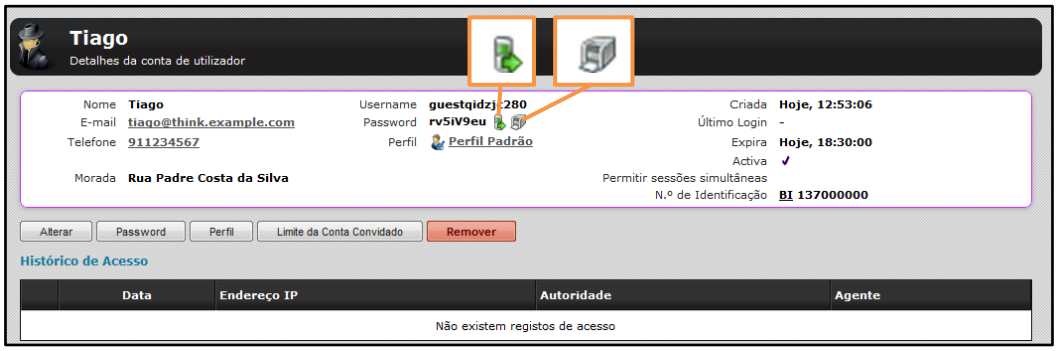


Neste ecrã pode escolher como irá restringir a conta do utilizador convidado, por tempo limitado ou por uma data limite. A opção “Permitir sessões simultâneas” tem como propósito permitir sessões em diversos dispositivos do utilizador convidado, sem esta opção o utilizador convidado só poderá ter uma sessão activa num dispositivo de cada vez.

Limite da Conta Convidado
Definir um limite para a conta de utilizador convidado
Restringir conta por tempo limitado
Coloque a duração em HH:MM que o utilizador convidado poderá usufruir a partir do momento que inicie sessão
Duração *
03:00
Restringir conta até uma data limite
Coloque a data e hora limite até à qual o utilizador poderá aceder utilizando esta conta
Data/Hora
04-04-2011
18:30
Permitir que a conta inicie sessão em diversos dispositivos ao mesmo tempo. Sem esta opção, quando a conta inicia sessão num dispositivo, bloqueará automaticamente outros dispositivos que tenham sido desbloqueados com esta sessão.
Permitir sessões simultâneas
Seguinte

No final, o NAC apresenta um ecrã com os detalhes da conta convidado com várias opções de configuração. O “Username” e a “Password” do utilizador são geradas automaticamente pelo NAC. Na imagem abaixo, junto ao campo “Password” encontram-se dois ícones. Estes ícones têm como função informar o utilizador convidado do seu “Username” e da sua “Password” para

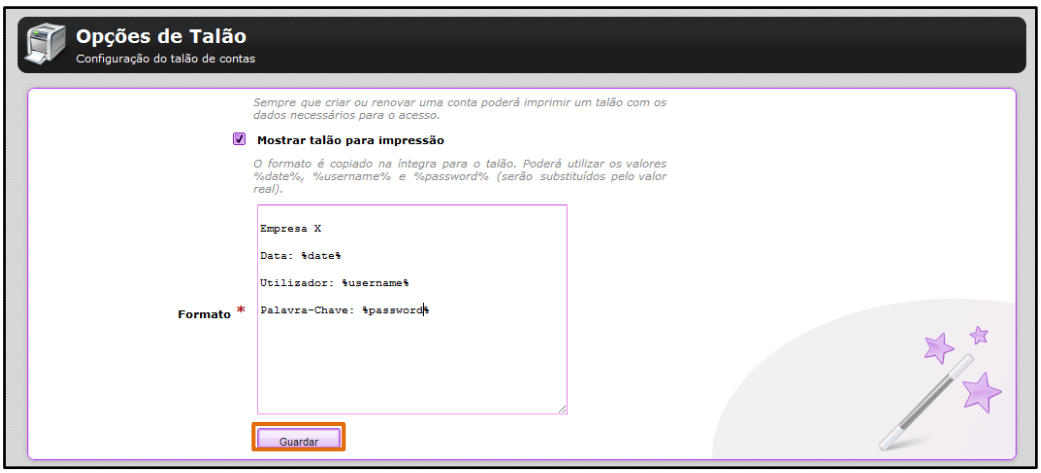
acederem á rede. O primeiro ícone permite enviar um SMS para o número de telemóvel do utilizador convidado com as respectivas informações. O segundo ícone imprime um talão com as respectivas informações mas primeiro é necessário configurar os talões.



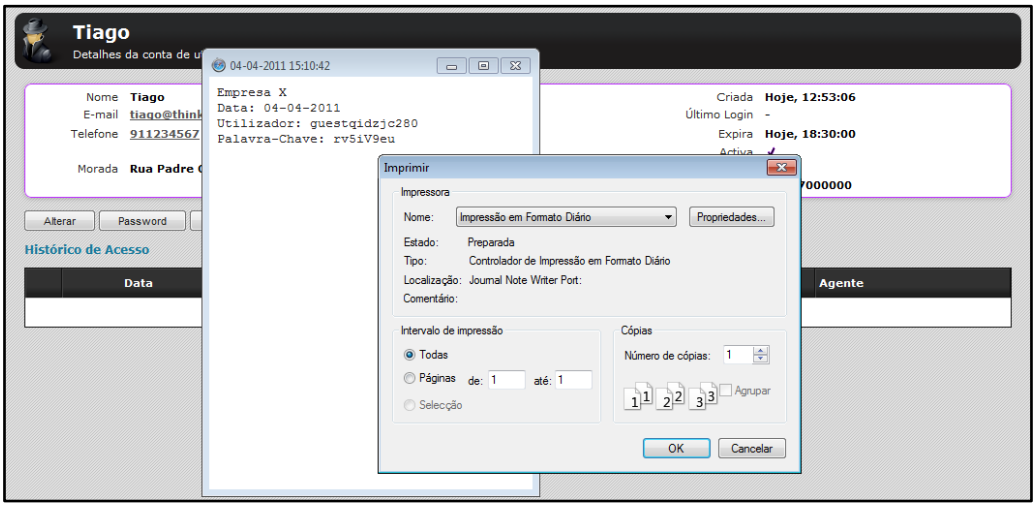
Nota: O prefixo do "username" pode ser configurado, a predefinição do NAC é a palavra "guest", neste caso o utilizador ficou "guestqidzjc280".

Para configurar as opções dos talões seleccione a opção "NAC" no ecrã de início e de seguida escolha a opção "Opções de Talão":

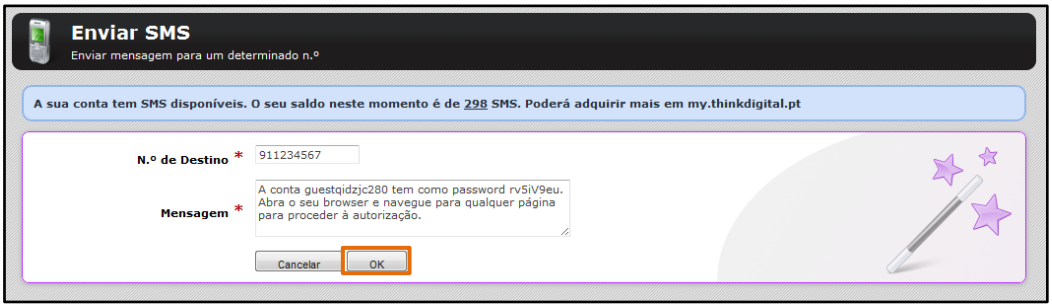
Para activar a funcionalidade de imprimir talões seleccione a opção "Mostrar talão para impressão" e preencha o campo "Formato". No campo "Formato" é possível utilizar três valores no talão, como se pode observar na imagem abaixo: "username", "password" e "date". Clique no botão "Guardar" para guardar as opções do talão.


Opções de Talão
Configuração do talão de contas
Sempre que criar ou renovar uma conta poderá imprimir um talão com os dados necessários para o acesso.
Mostrar talão para impressão
O formato é copiado na íntegra para o talão. Poderá utilizar os valores %date%, %username% e %password% (serão substituídos pelo valor real).
Formato *
Empresa X
Data: %date%
Utilizador: %username%
Palavra-Chave: %password%
Guardar

Com as configurações do talão guardadas, já pode ir a qualquer utilizador e imprimir um talão. Ao clicar no botão para imprimir o talão, o NAC abre uma janela com o talão e automaticamente "chama" a janela das configurações de impressão do browser.

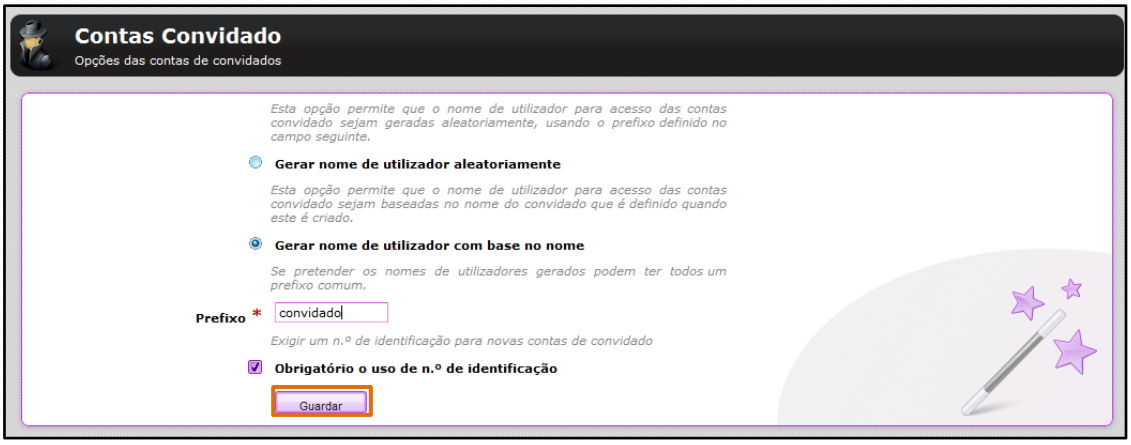


Se utilizar a opção "Enviar SMS", o NAC irá gerar um SMS com o "username" e com a "password" mas poderá editar o SMS ao seu gosto. Para enviar, clique no botão "Ok":


Enviar SMS
Enviar mensagem para um determinado n.º
A sua conta tem SMS disponíveis. O seu saldo neste momento é de 298 SMS. Poderá adquirir mais em my.thinkdigital.pt
N.º de Destino *
911234567
Mensagem *
A conta guestqidzjc280 tem como password rv5iV9eu. Abra o seu browser e navegue para qualquer página para proceder à autorização.
Cancelar
OK

Para alterar o funcionamento da geração dos "usernames" dos utilizadores convidados seleccione a opção "NAC" no ecrã de início e de seguida a opção "Contas Convidado":

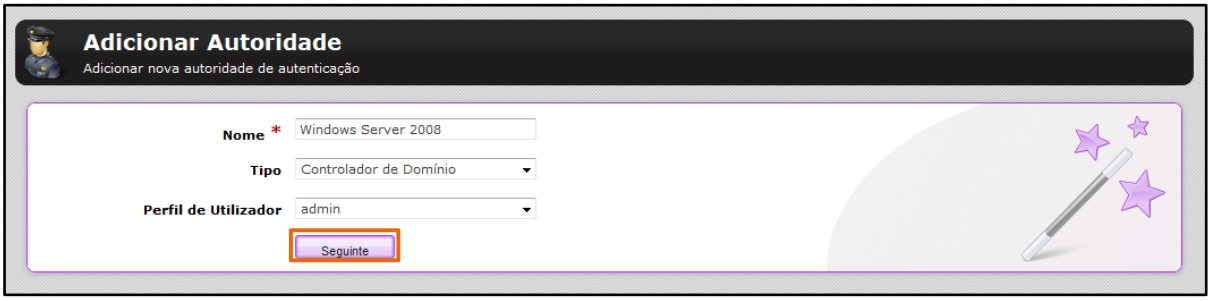
No ecrã "Contas Convidado" pode escolher se quer que o nome seja gerado aleatoriamente ou se é gerado com base no nome do utilizador. No campo "Prefixo" pode mudar a predefinição "guest" para outro prefixo á sua escolha.


Contas Convidado
Opções das contas de convidados
Esta opção permite que o nome de utilizador para acesso das contas convidado sejam geradas aleatoriamente, usando o prefixo definido no campo seguinte.
Gerar nome de utilizador aleatoriamente
Esta opção permite que o nome de utilizador para acesso das contas convidado sejam baseadas no nome do convidado que é definido quando este é criado.
Gerar nome de utilizador com base no nome
Se pretender os nomes de utilizadores gerados podem ter todos um prefixo comum.
Prefixo *
convidado
Exigir um n.º de identificação para novas contas de convidado
Obrigatório o uso de n.º de identificação
Guardar

5.4. Configurar Autoridades de Autenticação

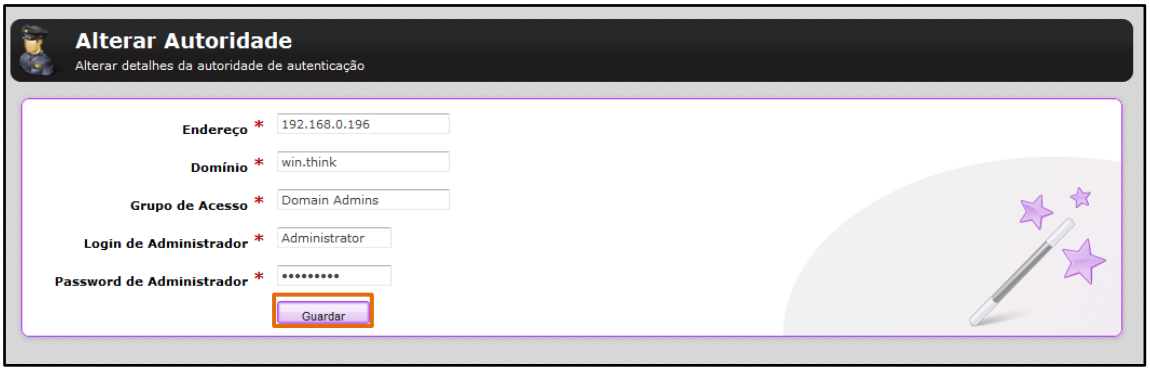
As Autoridades no NAC compreendem a utilização de autenticadores externos ao NAC, ou seja, é possível utilizar um controlador de domínio, como por exemplo controladores de domínio Windows, para os utilizadores desse domínio poderem autenticar-se no NAC com as credenciais que possuem no domínio. Existem três tipos de autenticadores possíveis de serem utilizados no NAC: controladores de domínio, servidores RADIUS e também outros servidores NAC. Para adicionar uma autoridade ao NAC, no ecrã “Politicas de Acesso” clique na opção “Autoridades” e de seguida clique na opção “Adicionar Autoridade” no menu “Atalhos”.

Preencha o nome desejado para a autoridade e escolha o tipo de autoridade a adicionar e o perfil a aplicar sobre os utilizadores dessa autoridade:

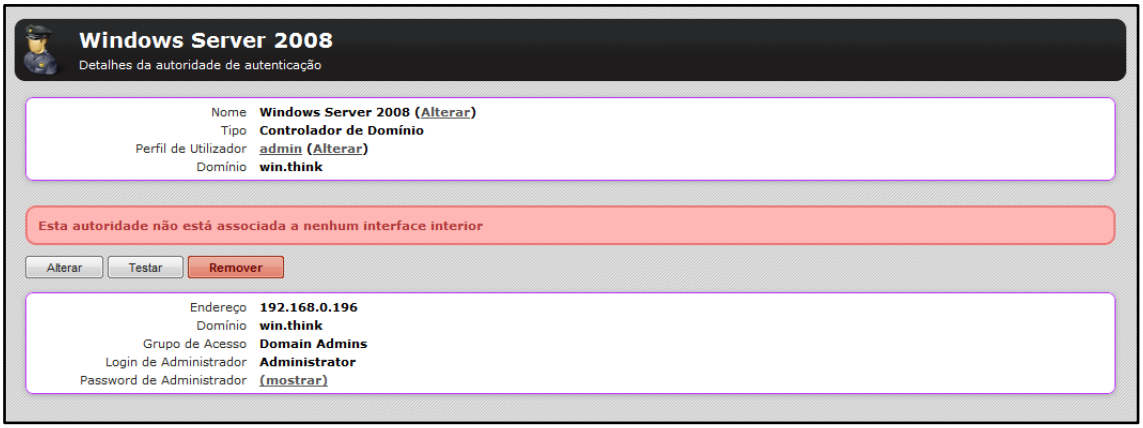


Neste ecrã é necessário preencher o campo “Endereço” que será o endereço do controlador de domínio, no campo “Domínio” preencha com o nome do domínio do seu controlador de domínio

e no campo “Grupo de Acesso” preencha com o nome do grupo a que os utilizadores pertencem. Por fim, no campo “Login de Administrador” e “Password de Administrador” é necessário introduzir o login e a password do utilizador que tem permissões para gerir o domínio.

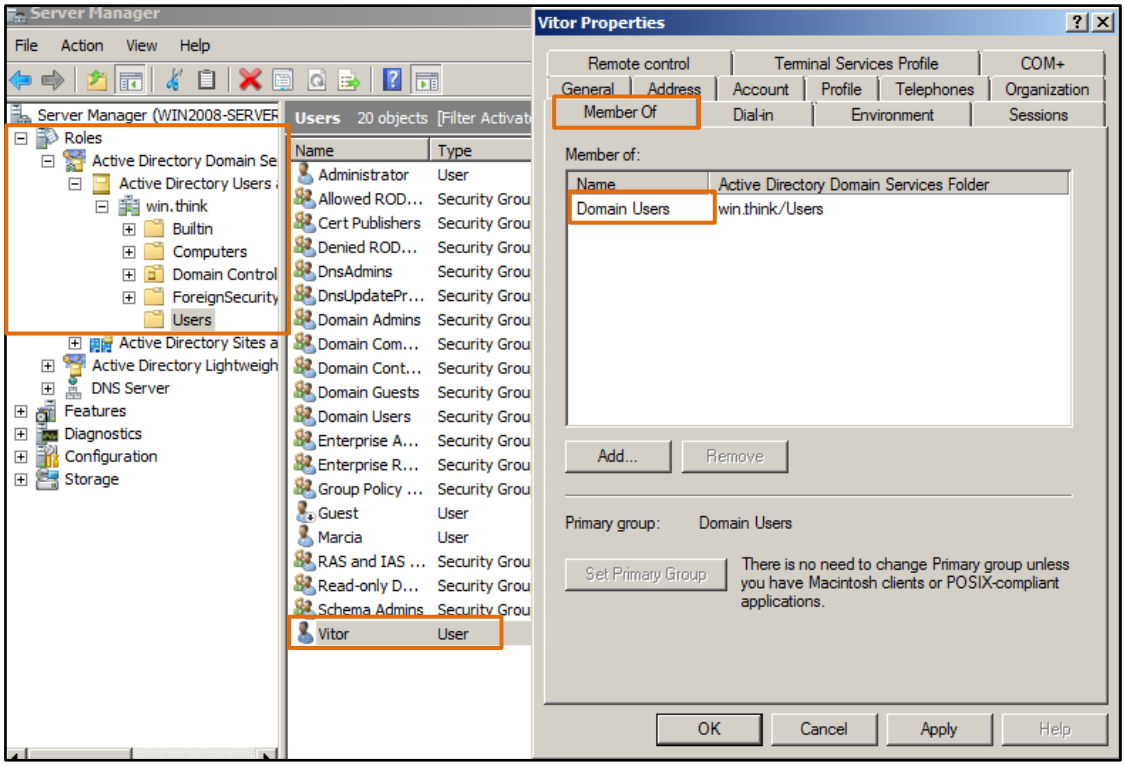


Como neste ecrã se pode verificar, é necessário associar a autoridade criada a um “Interface Interior”, só assim funcionará a autoridade. Adiante é explicado com mais detalhe os “Interfaces de Rede” do NAC.

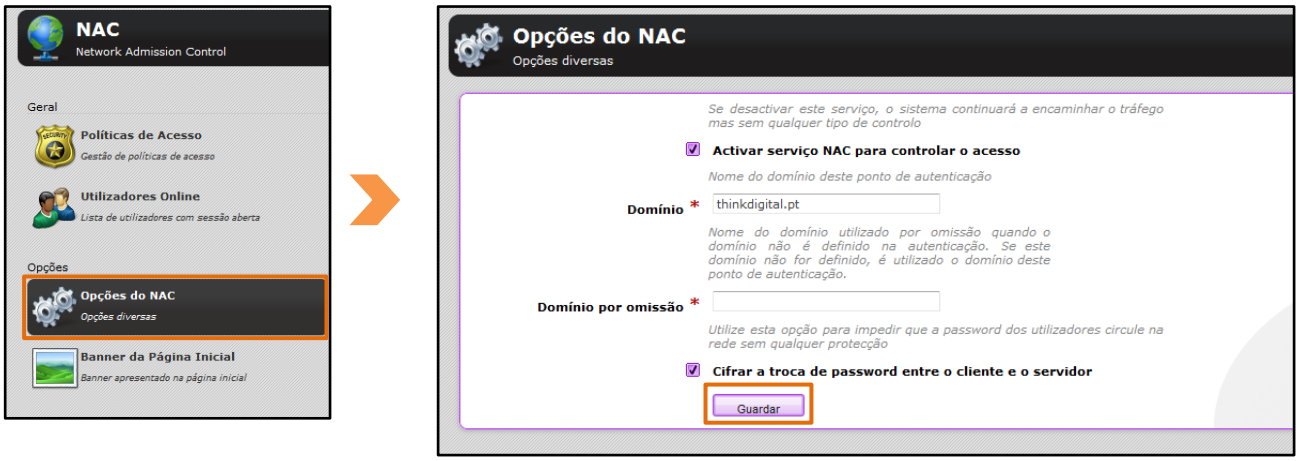


Para saber como associar uma autoridade de autenticação a um interface interior, vá até ao ponto “5.5. Opções Politicas de Acesso”.

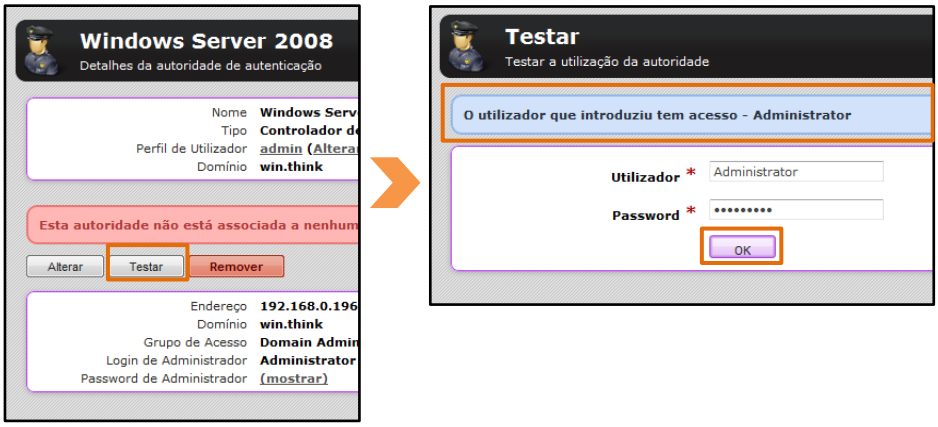
Se não souber a que grupo de acesso pertence um utilizador, no caso do Windows Server 2008, vá ao “Server Manager”, navegue até aos utilizadores e clique com lado direito do rato e seleccione a opção “Propriedades” e de seguida seleccione o separador “Membro de”.



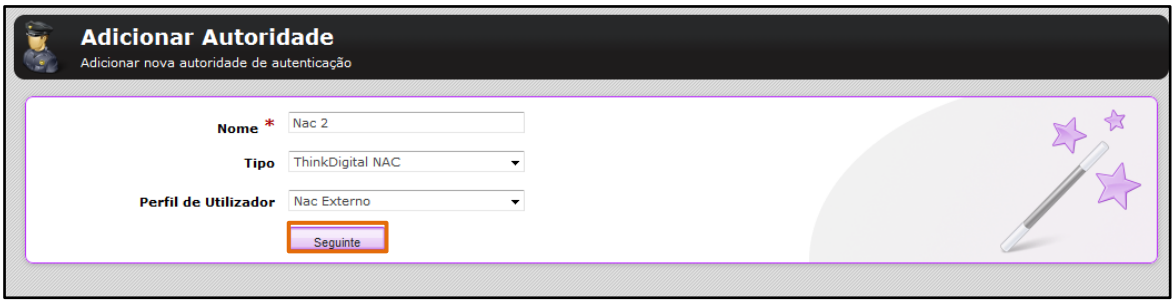
Para finalizar o processo, é necessário activar o NAC para controlar o acesso. Para activar seleccione a opção “Opções do NAC” no ecrã “NAC” e de seguida seleccione a opção “Activar serviço NAC para controlar acesso”. O campo “Domínio” é o domínio do NAC e no campo “Domínio por omissão” pode escolher colocar um domínio, por exemplo o da autoridade de autenticação que foi adicionado, para que os utilizadores não necessitem de escrever o domínio no momento da autenticação.


NAC
Network Admission Control
Geral
Políticas de Acesso
Gestão de políticas de acesso
Utilizadores Online
Lista de utilizadores com sessão aberta
Opções
Opções do NAC
Opções diversas
Banner da Página Inicial
Banner apresentado na página inicial
Opções do NAC
Opções diversas
Se desactivar este serviço, o sistema continuará a encaminhar o tráfego mas sem qualquer tipo de controlo
Activar serviço NAC para controlar o acesso
Nome do domínio deste ponto de autenticação
Domínio * thinkdigital.pt
Nome do domínio utilizado por omissão quando o domínio não é definido na autenticação. Se este domínio não for definido, é utilizado o domínio deste ponto de autenticação.
Domínio por omissão *
Utilize esta opção para impedir que a password dos utilizadores circule na rede sem qualquer protecção
Cifrar a troca de password entre o cliente e o servidor
Guardar

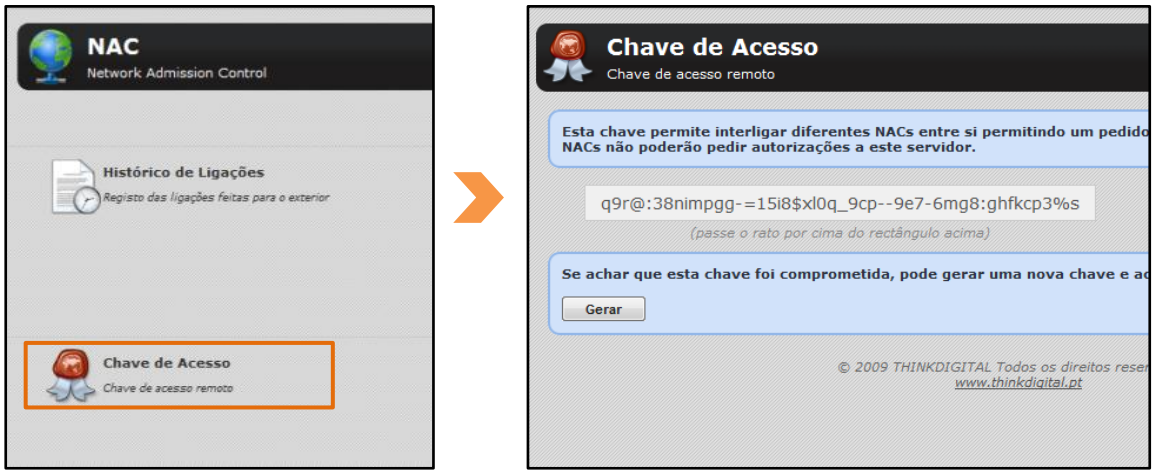
Por fim, para verificar se a autoridade de autenticação está a funcionar, volte aos detalhes da autoridade de autenticação e seleccione a opção “Testar”. No ecrã “Testar”, preencha os campos com o utilizador e a password de um utilizador pertencente ao grupo de acesso, neste caso “Domain Admins” e clique no botão “Ok”. Neste caso, como a mensagem indica na imagem abaixo indicada, o utilizador tem acesso.

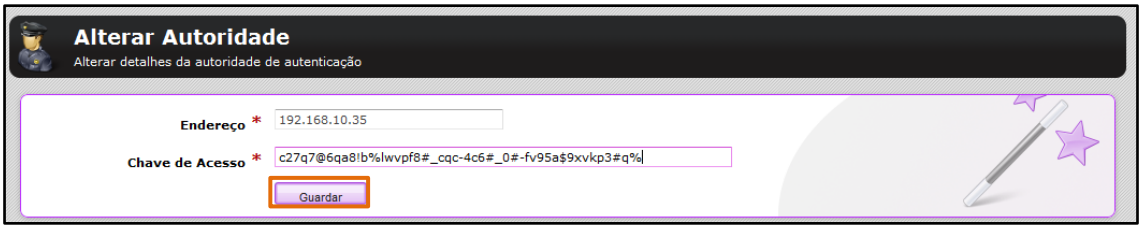


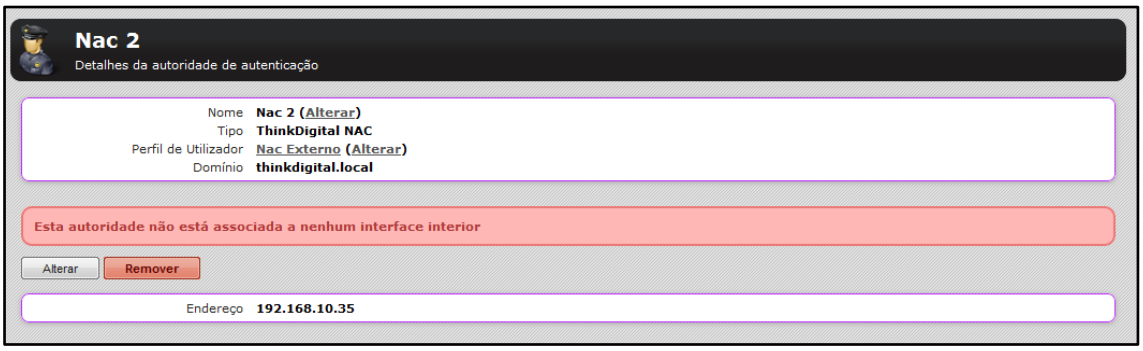
Para configurar um segundo NAC como autoridade de autenticação o processo é semelhante. No ecrã "Adicionar Autoridade", seleccione a opção "ThinkDigital NAC" no campo "Tipo" e preencha os campos restantes correctamente:



De seguida introduza o IP do NAC a adicionar no campo "Endereço" e no campo "Chave de Acesso" introduza a chave de acesso do NAC que quer adicionar. Para aceder a chave de acesso de um NAC, seleccione a opção "Chave de Acesso" no ecrã "NAC".


NAC
Network Admission Control
Histórico de Ligações
Registo das ligações feitas para o exterior
Chave de Acesso
Chave de acesso remoto
Chave de Acesso
Chave de acesso remoto
Esta chave permite interligar diferentes NACs entre si permitindo um pedido
NACs não poderão pedir autorizações a este servidor.
q9r@:38nimpgg-=15i8$xl0q_9cp--9e7-6mg8:ghfkcp3%s
(passe o rato por cima do rectângulo acima)
Se achar que esta chave foi comprometida, pode gerar uma nova chave e ac
Gerar
© 2009 THINKDIGITAL Todos os direitos reser
www.thinkdigital.pt

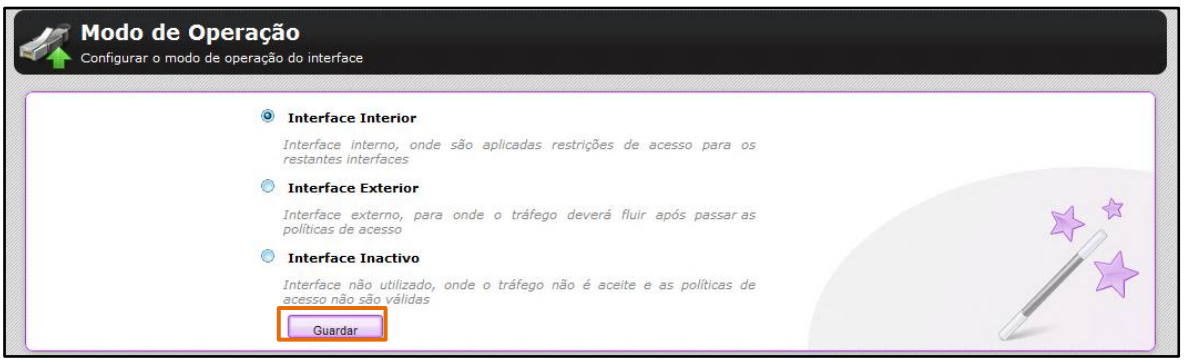


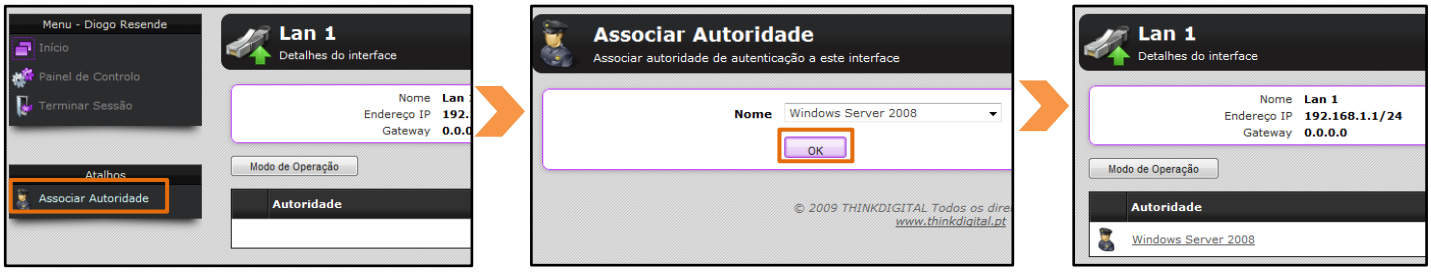


5.5. Opções Politicas de Acesso

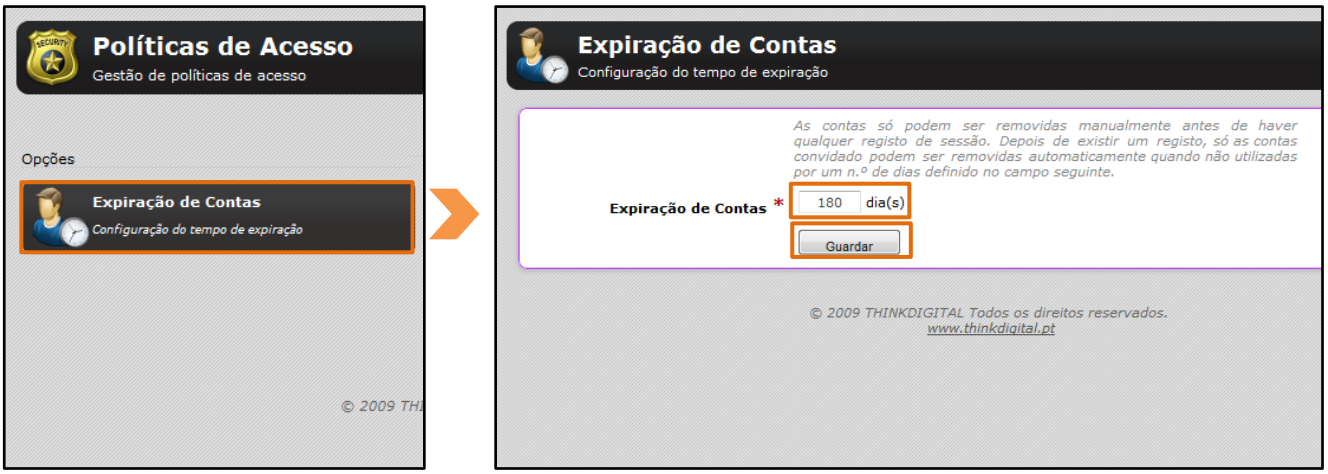
Existem três opções no ecrã “Políticas de Acesso”: “Interfaces de Rede”, “Expiração de Contas”, “Aplicar Regras”. Na opção “Interfaces de Rede” é possível configurar o modo de operação de cada interface de rede. Existem três modos: interface interior (onde são aplicadas restrições de acesso para os restantes interfaces), interface exterior (para onde o tráfego será direccionado depois de ser sujeito ás politicas de acesso) e interface inactivo. Para aceder a esta opção seleccione “Interfaces de Rede” no ecrã “Políticas de Acesso”. De seguida seleccione o interface a configurar e clique no botão “Modo de Operação”:

Por fim seleccione o modo desejado e clique no botão “Guardar”:


Modo de Operação
Configurar o modo de operação do interface
Interface Interior
Interface interno, onde são aplicadas restrições de acesso para os restantes interfaces
Interface Exterior
Interface externo, para onde o tráfego deverá fluir após passar as políticas de acesso
Interface Inactivo
Interface não utilizado, onde o tráfego não é aceite e as políticas de acesso não são válidas
Guardar



A opção “Expiração de Contas” permite que as contas que tenham qualquer registo de sessão só possam ser removidas passado um número de dias aqui definido. No caso dos utilizadores convidados, passado esse número de dias a conta será removida automaticamente. Para configurar esta opção seleccione a opção “Expiração de Contas” no ecrã “Politicas de Acesso” e de seguida preencha o campo “Expiração de Contas” com o número de dias desejado e clique no botão “Guardar”.


Políticas de Acesso
Gestão de políticas de acesso
Opções
Expiração de Contas
Configuração do tempo de expiração
© 2009 TH
Expiração de Contas
Configuração do tempo de expiração
As contas só podem ser removidas manualmente antes de haver qualquer registo de sessão. Depois de existir um registo, só as contas convidado podem ser removidas automaticamente quando não utilizadas por um n.º de dias definido no campo seguinte.
Expiração de Contas *
180
dia(s)
Guardar
© 2009 THINKDIGITAL Todos os direitos reservados.
www.thinkdigital.pt

A última opção, “Aplicar Regras”, tem como utilidade aplicar imediatamente todas as alterações feitas a nível de politicas de acesso, porque sempre que altera políticas de acesso o NAC demora cerca de um minuto a aplica-las. Por exemplo, a modificação de um perfil local não será aplicada imediatamente, se assim o desejar utilize esta opção. Para aplicar as configurações imediatamente seleccione a opção “Aplicar Regras” no ecrã “Políticas de Acesso” e de seguida clique no botão “Confirmar”.

5.6. Configurar Banner da Página Principal

Para adicionar um Banner á página principal seleccione a opção “Banner da Página Inicial” no ecrã “NAC”:

No ecrã seguinte pode escolher de que maneira poderá personalizar a página inicial, utilizando uma imagem, uma animação Adobe Flash ou um endereço de um site. Clique no botão “Guardas” para aplicar as modificações.

Para proseguir para o endereço que especificou é necessário que se autentique.
Username
Password
OK
Para sua segurança, a sua password é cifrada antes de ser enviada para o servidor.
Origem: 192.168.10.10
Destino: http://192.168.10.1/
THINKDIGITAL
Engenharia de Tecnologias de Informação

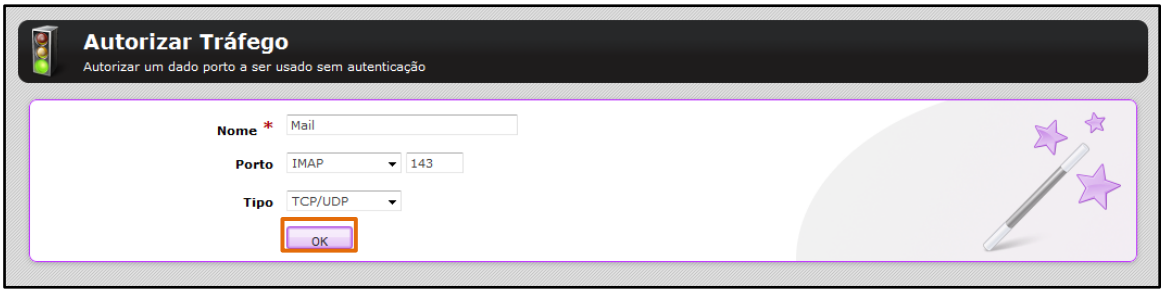
6. Menu Firewall

Este menu oferece a possibilidade de configurar Portos autorizados e não autorizados, configurar redireccionamentos de portos, configurar dispositivos privilegiados que não necessitam de autenticação ou até mesmo dispositivos excluídos que não terão acesso algum.

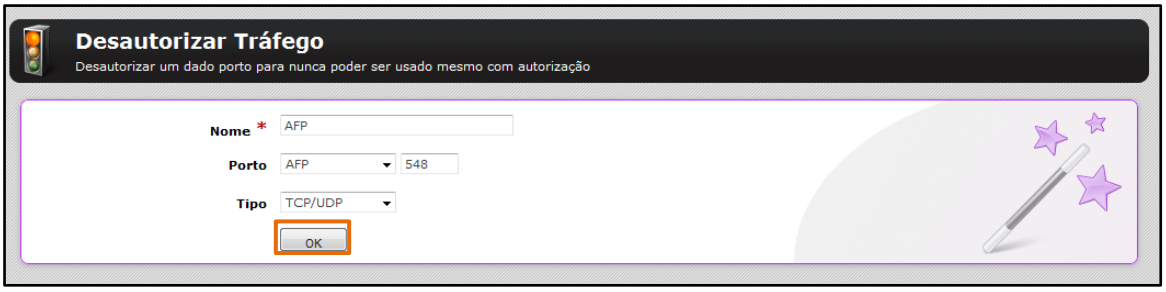
6.1. Configurar Tráfego Autorizado e Não Autorizado

Para configurar na Firewall do NAC portos autorizados é necessário seleccionar a opção “Firewall” no ecrã de inicial e seleccionar a opção “Tráfego Autorizado”. Para adicionar um porto autorizado clique na opção “Autorizar Tráfego” no menu “Atalhos”:

Para autorizar um porto escolha que porto quer autorizar no campo “Porto” e no campo “Tipo” escolha o tipo de protocolo de transporte a utilizar e clique no botão “Ok” para finalizar:



Para desautorizar tráfego, no ecrã “Firewall” clique na opção “Tráfego Não Autorizado” e de seguida clique na opção “Desautorizar Tráfego” no menu “Atalhos”. Proceda ao preenchimento dos campos da mesma forma como acima descrito na autorização de tráfego.



6.2. Criar Redireccionamentos

Os redireccionamentos têm como função redireccionar tráfego destinado a um porto para o dispositivo respectivo como por exemplo redireccionar o tráfego destinado para o porto 143 do protocolo IMAP para o servidor de e-mail. Para criar um redireccionamento seleccione a opção “Firewall” no ecrã inicial, depois seleccione a opção “Redireccionamentos”. Por fim para criar um redireccionamento clique na opção “Criar Redireccionamento” no menu “Atalhos”.

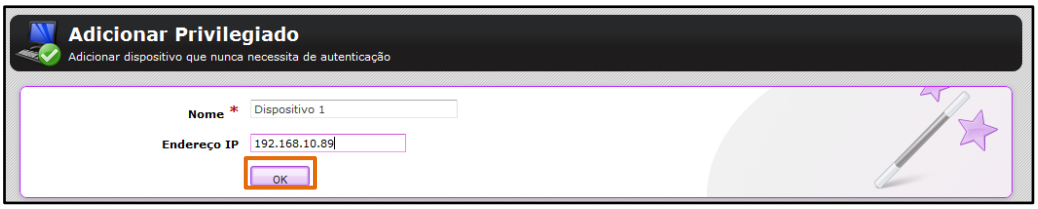
Preencha o campo “Porto” com o protocolo e a porta que deseja redireccionar e no campo “Redireccionar para” escreva o IP e o porto do dispositivo que receberá o tráfego. Para finalizar clique no botão “Ok”:

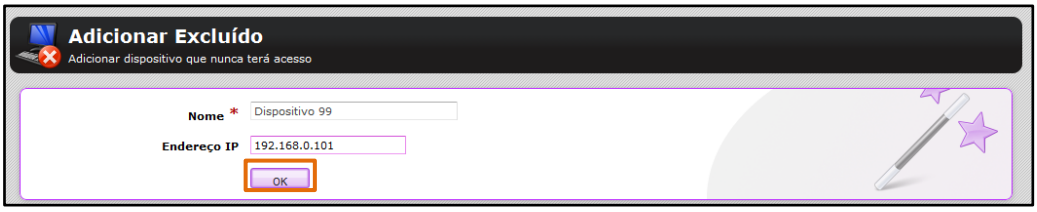
6.3. Dispositivos Privilegiados e Dispositivos Excluídos

Os dispositivos privilegiados e excluído no NAC tem como função garantir acesso sem autenticação para os dispositivos privilegiados e garantir que os dispositivos excluídos não tenham qualquer acesso á rede. Para adicionar um dispositivo privilegiado comece por seleccionar a opção “Firewall” no ecrã inicial e de seguida seleccionar a opção “Dispositivos Privilegiados”. Por fim clique na opção “Adicionar Privilegiado”.

No ecrã “Adicionar Privilegiado” preencha o nome que desejar para o dispositivo privilegiado e o endereço IP do dispositivo e clique no botão “Ok” para finalizar. Para adicionar um

dispositivo excluído basta seguir o mesmo processo do dispositivo privilegiado mas seleccionando a respectiva opção no ecrã “Firewall”.





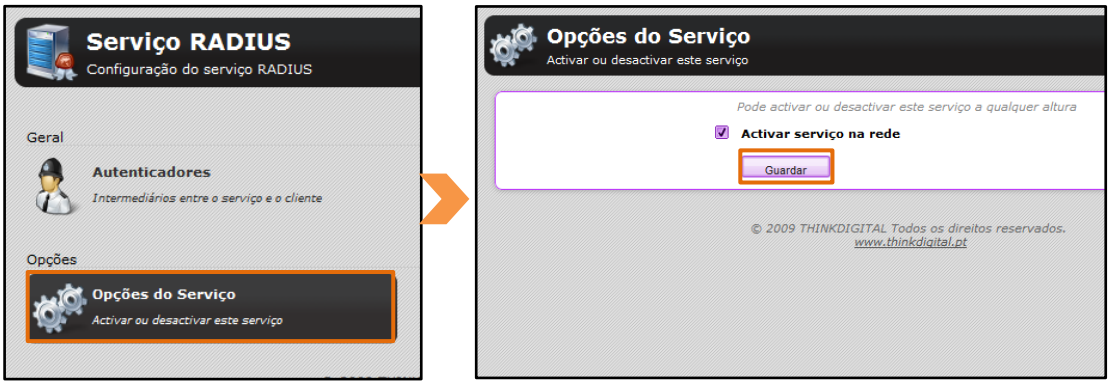
7. Menu Serviço RADIUS

No menu “Serviço RADIUS” é possível adicionar autenticadores RADIUS como um Access Point (AP) por exemplo. Para adicionar um autenticador RADIUS seleccione a opção “Serviço RADIUS” no ecrã inicial, seleccione depois a opção “Autenticadores” e por fim clique na opção “Criar Autenticador”.

No ecrã “Criar Autenticador” preencha o campo “Nome” com nome desejado, no campo “Identificador” escreva o nome do identificador, se for a um AP coloque o SSID utilizado na rede. No campo “Rede” escreva o endereço da rede na notação CIDR e no campo “Password” preencha com a palavra-chave da rede. Por fim clique no botão “Ok” para finalizar.

Criar Autenticador
Criar um autenticador para o serviço
Nome * AP ThinkDigital
No caso de um AP, coloque o SSID utilizado na rede
Identificador * ThinkDigital-AP
Utilize a notação CIDR (se quiser restringir a um endereço IP, utilize a notação w.x.y.z/32)
Rede * 192.168.0.0/24
Password *
OK

Depois de ter criado um autenticador é necessário activar o serviço RADIUS. Para activar seleccione a opção “Opções do Serviço” no ecrã serviço RADIUS, de seguida seleccione a opção “Activar serviço na rede” e clique no botão “Guardar”.

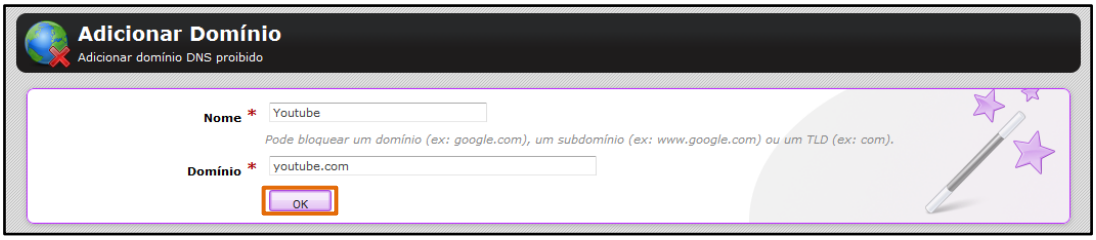


8. Menu Proxy HTTP

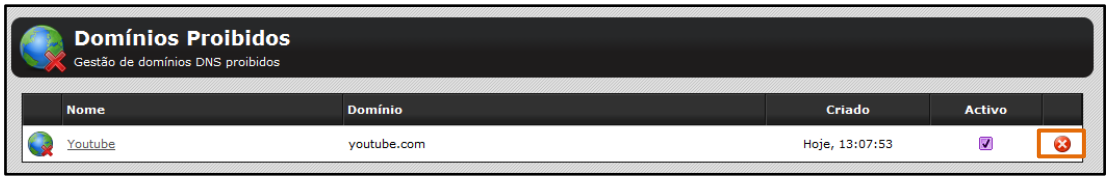
O NAC possui uma proxy transparente na qual pode configurar domínios proibidos para barrar acesso, como por exemplo barrar acesso ao domínio “youtube.com” e também pode visualizar domínios visitados. A proxy do NAC faz uso de cache, sendo configurável o seu tamanho.

Para gerir e adicionar domínios proibidos seleccione a opção “Proxy HTTP” no ecrã inicial, de seguida seleccione a opção “Domínios Proibidos” e por fim seleccione na opção “Adicionar Domínio” no menu “Atalhos”.

No ecrã “Adicionar Domínio” preencha no campo “Nome” com um nome desejado para identificar o domínio e no campo “Domínio” escreva o domínio a bloquear o acesso, neste caso “youtube.com”, finalizando o processo com um clique no botão “Ok”.



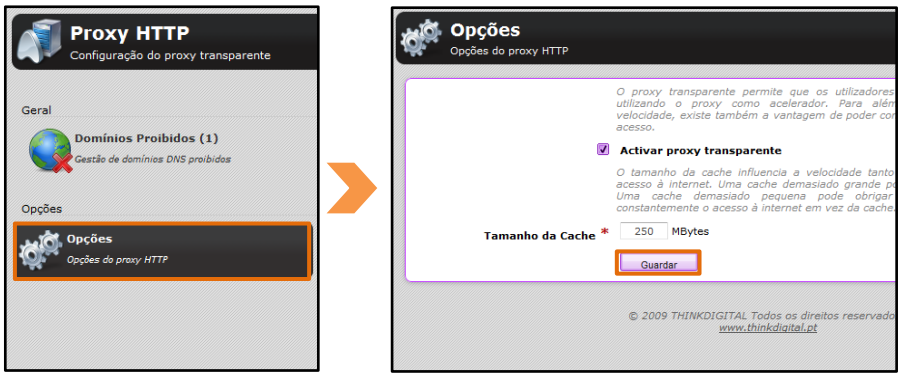
Neste ecrã pode visualizar todos os domínios proibidos assim como remover domínios se o desejar seleccionando o botão vermelho abaixo indicado.



Para visualizar domínios já visitados, no ecrã “Proxy HTTP” seleccione a opção “Domínios Visitados”. No ecrã “Domínios Visitados” pode pesquisar os domínios visitados, para isso escreva o domínio pretendido no campo “Filtrar” e clique no botão “Ok”. Este ecrã também lhe dá a possibilidade de proibir domínios directamente seleccionando o botão vermelho correspondente ao domínio desejado.

Proxy HTTP
Configuração do proxy transparente
Geral
Domínios Visitados (228)
Visualização dos domínios já visitados
Opções
Estado do Serviço
Estatísticas do proxy HTTP
Domínios Visitados
Visualização dos domínios já visitados
Filtrar
google
OK
A mostrar 228 de 228 - 6 página(s)
Domínio
Tráfego
Alexa Top
Primeira vez
Última vez
Visitantes
v4.cache4.c.youtube.com 13.47 MiB - Ontem, 12:40:41 Ontem, 12:40:41 1
v22.lscache6.c.youtube.com 8.16 MiB - Ontem, 12:41:14 Ontem, 12:41:14 1
v23.nonxt5.c.youtube.com 5.41 MiB - Ontem, 12:42:04 Ontem, 12:42:04 1
in.pt 2.91 MiB - Ontem, 11:43:53 Ontem, 12:48:30 1
ubuntu.com 1.34 MiB - Ontem, 12:53:10 Ontem, 12:53:10 1
uaonline.ua.pt 1.10 MiB - Ontem, 11:50:58 Ontem, 11:50:58 1
viaverde.pt 1.01 MiB - Ontem, 12:17:58 Ontem, 12:17:58 1
microsoft.com 946.63 KiB - Ontem, 11:48:33 Ontem, 11:53:53 1
i.s.sl.pt 738.08 KiB - Ontem, 11:58:02 Ontem, 12:08:02 1
portugal.com 615.28 KiB - Ontem, 11:46:20 Ontem, 11:46:20 1
google.pt 606.35 KiB - Dia 11, 18:25:26 Ontem, 12:38:02 1
mail.thinkdigital.pt 498.72 KiB - Ontem, 11:41:40 Ontem, 12:52:17 1

Por fim, para activar a proxy e configurar o tamanho da cache seleccione “Opções” no ecrã “Proxy HTTP”, de seguida seleccione a opção “Activar proxy transparente” e no campo “Tamanho da Cache” escolha o tamanho que a cache da proxy irá ter. Não se esqueça que muito pouca cache obrigará a proxy a usar constantemente o acesso a internet em vez da cache, e uma cache muito grande irá diminuir a performance da proxy.

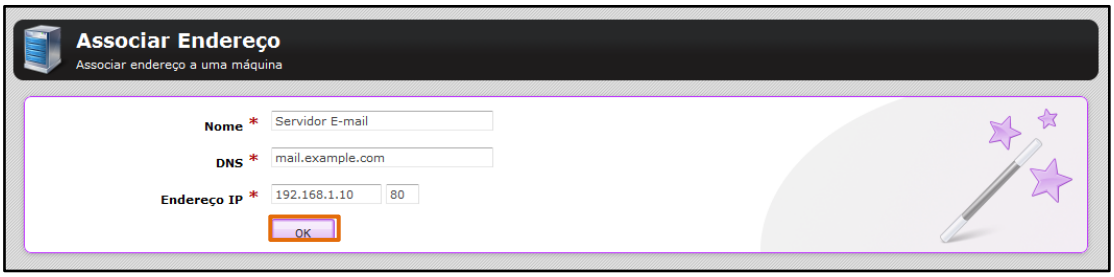


Para visualizar tráfego realizado seleccione a opção “Estado do Serviço” no ecrã “Proxy HTTP”. Pode visualizar por exemplo o tráfego realizado nas últimas horas ou por dia da semana, seleccionando o separador correspondente.

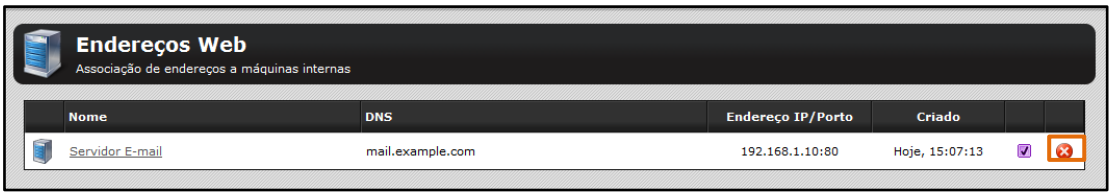
9. Menu Reverse Proxy

Como o nome indica, o menu “Reverse Proxy” que trabalhar no sentido contrário ao da proxy transparente. É uma proxy que recebe pedidos de clientes externos á rede, redireccionando-os para os servidores respectivos. Para isso é necessário associar um endereço ao endereço IP da máquina respectiva. Comece por seleccionar a opção “Reverse Proxy” no ecrã inicial, de seguida seleccione a opção “Endereços Web” e por fim clique na opção “Associar Endereço” no menu “Atalhos”:

Preencher o campo “Nome” com o nome desejado, o campo “Endereço IP” preencha com o endereço IP e o porto correspondente á máquina para a qual deseja redireccionar os pedidos, e o campo “DNS” com o endereço.



Se necessitar de eliminar uma associação clique no botão vermelho abaixo indicado:

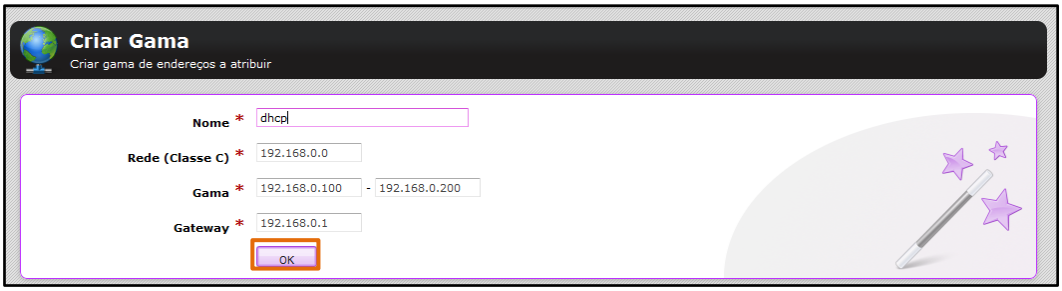


Por fim, o menu “Reverse Proxy” permite a configuração de endereço de “fallback” por omissão para quando um endereço não se encontra disponível. Para configurar um endereço de “fallback” no ecrã “Reverse Proxy” seleccione a opção “Fallback por Omissão”, de seguida preencha com o endereço IP e porto da máquina que será utilizada para o “fallback” e clique no botão “Ok”.

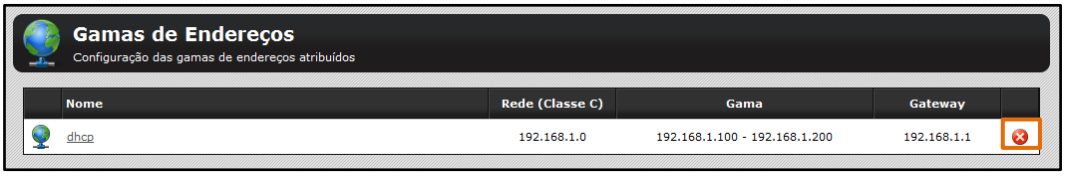
10. Menu Serviço DHCP

O serviço DCHP permite que o NAC possa criar e configurar uma gama de endereços, para assim os dispositivos na rede obterem um endereço IP, e restantes configurações de rede, automaticamente. Também permite a atribuição de IPs fixos a máquinas. Para configurar uma gama de endereços seleccione a opção “Serviço DHCP” no ecrã inicial, de seguida seleccione a opção “Gama de Endereços” e por fim clique na opção “Criar Gama”.

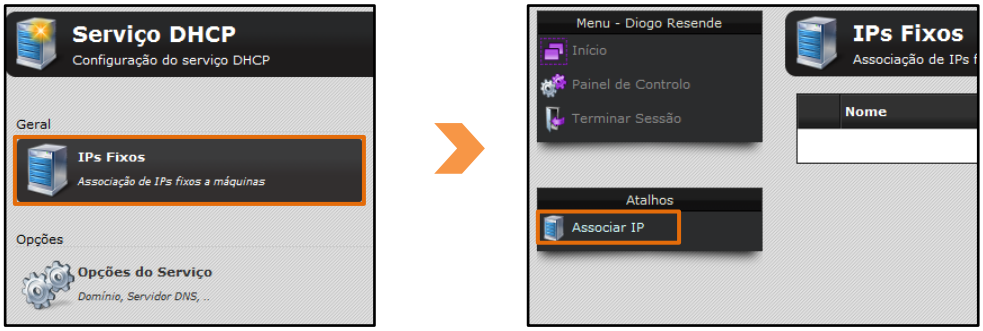
No ecrã “Criar Gama” preencha todos os campos correctamente e clique no botão “Ok” para finalizar, como se pode verificar na imagem abaixo:



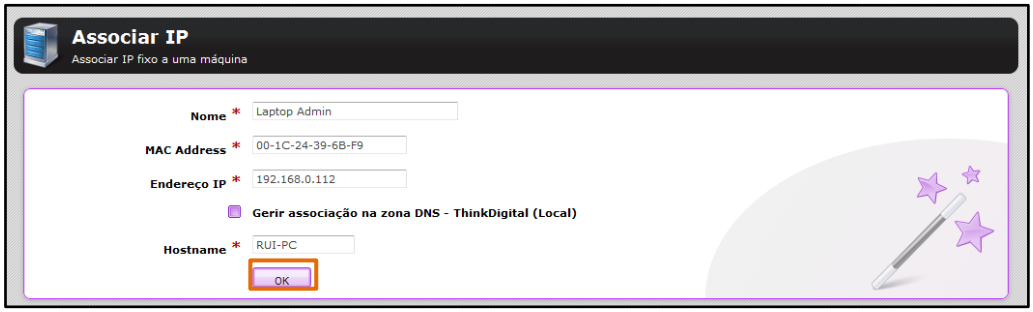
Quando existir necessidade de remover uma gama de endereço, clique no botão vermelho abaixo indicado na imagem.



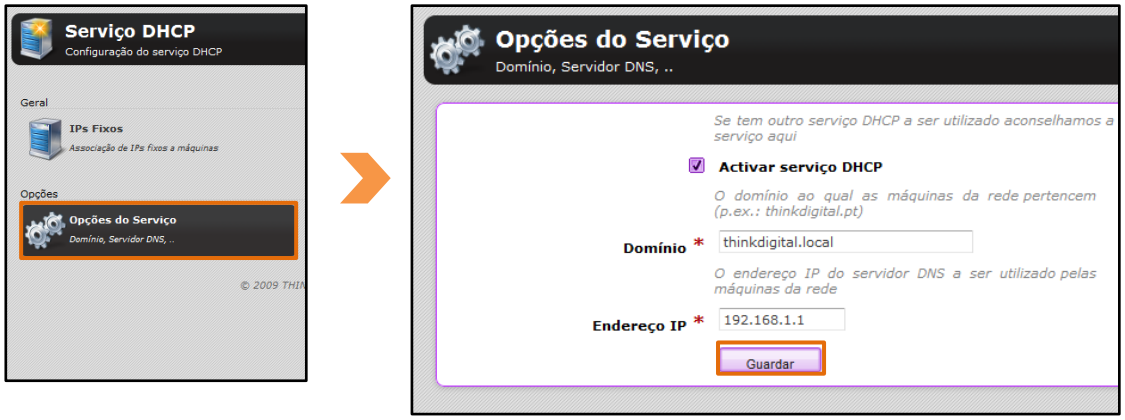
Para associar um IP a uma máquina seleccione opção “IPs Fixos” no ecrã “Serviço DHCP”



No ecrã “Associar IP” preencha todos os campos correctamente.


Associar IP
Associar IP fixo a uma máquina
Nome * Laptop Admin
MAC Address * 00-1C-24-39-6B-F9
Endereço IP * 192.168.0.112
Gerir associação na zona DNS - ThinkDigital (Local)
Hostname * RUI-PC
OK

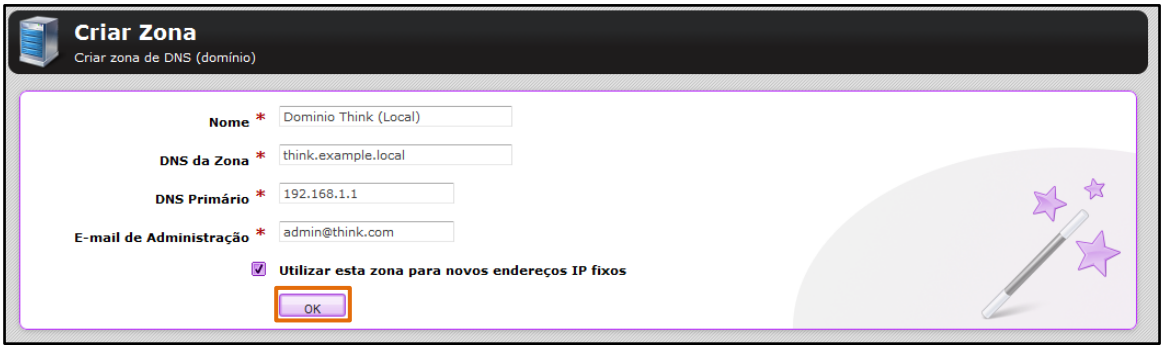
Por fim, para activar o serviço DHCP seleccione a opção “Opções do Serviço” e de seguida seleccione o campo “Activar serviço DHCP”, no campo “Domínio” preencha com o domínio ao qual as máquinas da rede pertencem e no campo “Endereço IP” preencha com o endereço IP do servidor DNS que as máquinas irão utilizar.


Serviço DHCP
Configuração do serviço DHCP
Geral
IPs Fixos
Associação de IPs fixos a máquinas
Opções
Opções do Serviço
Domínio, Servidor DNS, ..
Opções do Serviço
Domínio, Servidor DNS, ..
Se tem outro serviço DHCP a ser utilizado aconselhamos a serviço aqui
Activar serviço DHCP
O domínio ao qual as máquinas da rede pertencem (p.ex.: thinkdigital.pt)
Domínio *
thinkdigital.local
O endereço IP do servidor DNS a ser utilizado pelas máquinas da rede
Endereço IP *
192.168.1.1
Guardar

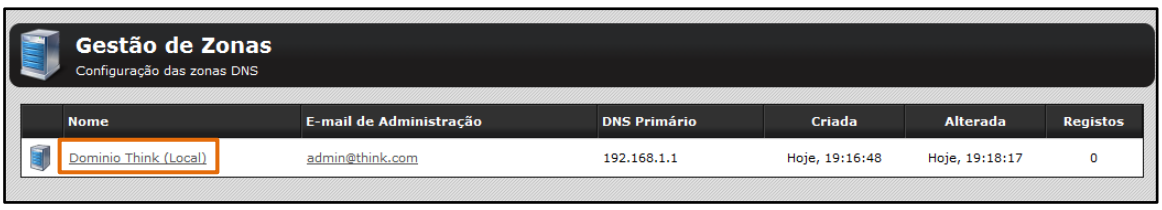
11. Menu Serviço DNS

No menu “Serviço DNS” é possível criar e gerir zonas DNS. A zona DNS é uma porção de informação do DNS global que contém parâmetros que permitem que os vários serviços do seu domínio sejam direccionados para as máquinas correctas que irão processar os pedidos. Para criar uma zona no NAC seleccione a opção “Serviço DNS” no ecrã inicial, de seguida seleccione a opção “Gestão de Zonas” e por fim clique na opção “Criar Zona” no menu “Atalhos”.

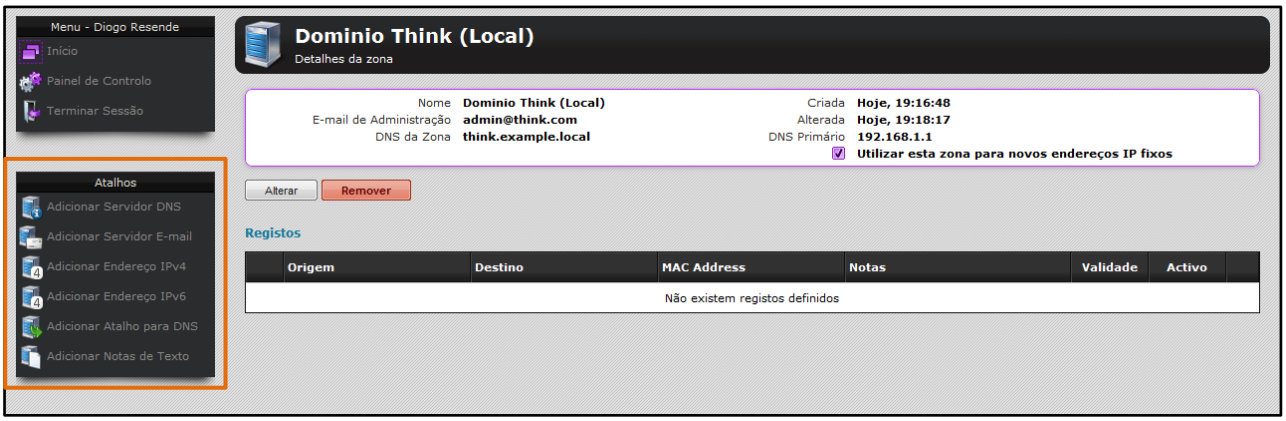
Preencha correctamente os campos, para finalizar seleccione o botão “Ok”.



Para gerir a zona criada clique no nome da zona.



No ecrã de gestão da zona é possível adicionar inúmeras funcionalidades á zona como se pode verificar no menu “Atalhos”.



THINKDIGITAL
HQ – Rua Cristóvão Pinho Queimado, nº65
MIRADOR BUSINESS CENTER
Aveiro – Portugal
Tf: +351 234 197 149
Fx: +351 234 197 562
www.thinkdigital.pt